

~~Sub~~
~~D~~ 5 What is claimed is:

1. A system for preventing tampering with signal conditioning circuitry in electronics that determines a parameter from signals received from sensors, said system comprising:
 - a host system that receives data from and send data to said signal conditioning circuitry;
 - a processing unit in said host system;
 - a memory connected to said processing unit;
 - instructions for directing said processing unit in said host system to periodically transmit a request for authentication information from said signal conditioning circuitry, receive said authentication information from said signal conditioning circuitry in response to said request, and store a record of said authentication information received from said signal conditioning circuitry in said memory; and
 - a media readable by said processing unit for storing said instructions.
2. The system of claim 1 wherein said authentication information includes a unique identification for said signal conditioning circuitry.
3. The system of claim 1 wherein said authentication information includes calibration data for said signal conditioning circuitry.
4. The system of claim 1 wherein said instructions for directing said processing unit in said host system includes:
 - instructions for directing said processing unit in said host system to compare said authentication information with initial information, and signal an error in response to said authentication information not being equal to said initial information.
5. The system of claim 4 wherein said instruction for directing said processing unit in said host system includes:
 - instructions for directing said processing unit in said host system to terminate operation of said system.

6. The system of claim 4 wherein said instructions include:
instructions for directing said processing unit to obtain said initial information.

7. The system of claim 6 wherein said instructions for directing said processing unit to obtain said initial information includes:

instructions for directing said processing unit in said host system to:
transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,
receive said authentication information from said signal conditioning circuitry, and
store said authentication information as said initial information in said memory.

8. The system of claim 1 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to compare said authentication information with initial information, and perform a programmed function in response to said authentication information not being equal to said initial information.

9. The system of claim 1 further comprising:

a processing unit in said signal conditioning circuitry;
a memory connected in said signal conditioning circuitry that stores said authentication information;

instructions for directing said processing unit in said signal conditioning circuitry to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

a media readable by said processing unit in said signal conditioning circuitry for storing said instructions.

Subj 105
10. The system of claim 1 wherein said record includes a time stamp indicating when said authentication information is received.

11. The system of claim 1 wherein said record includes said authentication information received from said signal conditioning circuitry.

12. Meter electronics for a Coriolis flowmeter that detects possible tampering comprising:

a host system that receives parameter signals indicating properties of a material flowing through said Coriolis flowmeter from said signal conditioner and supplies powers to signal conditioner;

5 a signal conditioner remote from said host system and communicatively connected to said host system wherein said signal conditioner receives pick-off signals from sensors affixed to said Coriolis flowmeter and generates said parameter signals from said pick-off signals;

10 a processing unit in said host system;

a memory connected to said processing unit in said host system;

instructions for directing said processing unit in said host system to:

15 periodically transmit a request for authentication information to said signal conditioner,

receive said authentication information from said signal conditioner in response to said request, and

store said authentication information in said memory; and

a media readable by said processing unit for storing said instructions.

13. The meter electronics of claim 12 wherein said authentication information includes a unique identification for said signal conditioner.

14. The meter electronics of claim 12 wherein said authentication information includes calibration data for said signal conditioner.

Subj 105
15. The meter electronics of claim 12 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

5 compare said authentication information with initial information, and

signal an error in response to said authentication information not being equal to said initial information.

16. The meter electronics of claim 15 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to terminate operation of said system.

17. The meter electronics of claim 16 wherein said instructions include:

instructions for directing said processing unit to obtain said initial information.

18. The meter electronics of claim 17 wherein said instructions for directing said processing unit to obtain said initial information includes:

instructions for directing said processing unit in said host system to:

5 transmit a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry being connected to said host system,

receive said authentication information from said signal conditioning circuitry, and

10 store said authentication information as said initial information in said memory.

19. The meter electronics of claim 12 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

5 compare said authentication information with initial information, and

perform a programed function in response to said authentication information not being equal to said initial information.

20. The meter electronics of claim 12 further comprising:

a processing unit in said signal conditioner;

5 a memory connected in said signal conditioner that stores said authentication information;

10 instructions for directing said processing unit in said signal conditioner to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

15 a media readable by said processing unit in said signal conditioner for storing said instructions.

21. The meter electronics of claim 12 wherein said record includes a time stamp indicating when said authentication information is received.

22. The meter electronics of claim 12 wherein said record includes said authentication information received from said signal conditioner.

23. A Coriolis flowmeter having tamper resistant meter electronics comprising:
5 at least one flow tube through which material flows;
a driver affixed to said at least one flow tube that vibrates said at least one flow tube as said material flows through said at least one flow tube;
sensors affixed to at least two different points of said at least one flow tube to generate sensor signals indicating vibrations of said at least one flow tube at said at least two different points;

10 a signal conditioner that transmits a drive signal to said driver, receives said sensors signals, and generates parameter signals from said sensors signals wherein said parameter signals indicate a property of said material;

a host system that provides power to said signal conditioner and receives said parameter signals from said signal conditioner;

a processing unit in said host system;

a memory connected to said processing unit in said host system;

15 instructions for directing said processing unit in said host system to:

periodically transmit a request for authentication information to said signal conditioner,

receive said authentication information from said signal conditioner in

20 response to said request, and

store said authentication information in said memory; and
a media readable by said processing unit for storing said instructions.

~~24. The Coriolis flowmeter of claim 23 wherein said authentication information includes a unique identification for said signal conditioner.~~

~~25. The Coriolis flowmeter of claim 23 wherein said authentication information includes calibration data for said signal conditioner.~~

~~26. The Coriolis flowmeter of claim 23 wherein said instructions for directing said processing unit in said host system includes:~~

~~instructions for directing said processing unit in said host system to:
compare said authentication information with initial information, and
signal an error in response to said authentication information not being
equal to said initial information.~~

~~27. The Coriolis flowmeter of claim 26 wherein said instructions for directing said processing unit in said host system includes:~~

~~instructions for directing said processing unit in said host system to terminate
operation of said Coriolis flowmeter in response to said signal.~~

~~28. The Coriolis flowmeter of claim 26 wherein said instructions for directing said host system include:~~

~~instructions for directing said processing unit to obtain said initial information.~~

~~29. The Coriolis flowmeter of claim 28 wherein said instructions for directing said processing unit to obtain said initial information includes:~~

~~instructions for directing said processing unit in said host system to:~~

~~transmit a initialize request to said signal conditioning circuitry for said
authentication information in response to detecting said signal conditioning
circuitry being connected to said host system,~~

~~receive said authentication information from said signal conditioning~~

10 circuitry, and

store said authentication information as said initial information in said memory.

30. The Coriolis flowmeter of claim 23 wherein said instructions for directing said processing unit in said host system includes:

instructions for directing said processing unit in said host system to:

compare said authentication information with initial information, and

5 perform a programmed function in response to said authentication information not being equal to said initial information.

31. The Coriolis flowmeter of claim 23 further comprising:

a processing unit in said signal conditioner;

5 a memory connected in said signal conditioner that stores said authentication information;

instructions for directing said processing unit in said signal conditioner to receive said request for said authentication information, read said authentication information from said memory, and transmit said authentication information to said host system; and

10 a media readable by said processing unit in said signal conditioner for storing said instructions.

32. The Coriolis flowmeter of claim 23 wherein said record includes a time stamp indicating when said authentication information is received.

33. The Coriolis flowmeter of claim 23 wherein said record includes said authentication information received from said signal conditioner.

34. A method for preventing tampering with signal conditioning circuitry in a system comprising the steps of:

periodically transmitting a request for authentication information from a host system to said signal conditioner;

5 receiving said authentication information from said signal conditioning circuitry

in response to said request; and

storing said authentication information in a memory in said host system.

35. The method of claim 34 wherein said authentication information includes a unique identification for said signal conditioning circuitry.

36. The method of claim 34 wherein said authentication information includes calibration data for said signal conditioner.

37. The method of claim 34 further comprises the steps of:
comparing said authentication information with initial information stored in said host system; and
signaling an error in response to said authentication information not being equal to said initial information.

38. The method of claim 37 further comprises the steps of:
terminating operation of said system in response to said signal of said error.

39. The method of claim 38 further comprises the step of:
obtaining said initial information.

40. The method of claim 39 wherein said step of obtaining said initial information comprises the steps of:

transmitting a initialize request to said signal conditioning circuitry for said authentication information in response to detecting said signal conditioning circuitry

5 being connected to said host system;

receiving said authentication information from said signal conditioning circuitry;
and

storing said authentication information as said initial information in said memory.

41. The method of claim 34 further comprising the steps of:

receiving said request for said authentication information in said signal

conditioning circuitry;

reading said authentication information from a memory in said signal

5 conditioning circuitry; and

transmitting said authentication information to said host system.

~~42. The method of claim 34 wherein said record includes a time stamp indicating when said authentication information is received.~~

~~43. The method of claim 34 further comprises the steps of:~~

~~comparing said authentication information with initial information stored in said host system; and~~

~~performing a programmed function in response to said authentication~~

5 information not being equal to said initial information.